Journal of Number Theory 130 (2010) 2628–2633

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The algebraic independence of the sum of divisors functions ☆

Daniel Lustig

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104, United States

ARTICLE INFO

Article history:
Received 6 August 2009
Available online 3 August 2010
Communicated by Robert C. Vaughan

Keywords:
Algebraic independence
Sum of divisors
Perfect numbers

ABSTRACT

Let $\sigma_j(n) = \sum_{d|n} d^j$ be the sum of divisors function, and let I be the identity function. When considering only one input variable n, we show that the set of functions $\{\sigma_i\}_{i=0}^{\infty} \cup \{I\}$ is algebraically independent. With two input variables, we give a non-trivial identity involving the sum of divisors function, prove its uniqueness, and use it to prove that any perfect number n must have the form $n = r\sigma(r)/(2r - \sigma(r))$, with some restrictions on r. This generalizes the known forms for both even and odd perfect numbers.

1. Introduction

Let σ_j be the sum of divisors function $\sigma_j(n) = \sum_{d|n} d^j$. When not written, the subscript j is assumed to be equal to 1. We will investigate the algebraic dependence of these functions. When only one input variable n is considered, Bellman and Shapiro [1] show that σ_0, σ_1, and the identity function I, as well as Euler's totient function φ, the Möbius function μ, and the number of unitary divisors function σ_0^*, are all algebraically independent. We extend the first part of this result to include the sum of divisors function for all subscripts i.

Theorem 1. *The set of functions $\{\sigma_i\}_{i=0}^{\infty} \cup \{I\}$, where I is the identity function, is algebraically independent.*

We next consider the case of more than one input variable. There exist well-known identities of this form, such as

☆ This work was partially supported by a National Science Foundation grant.
E-mail address: lustigdj@alumni.upenn.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.03.022

$$\sum_{i=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)},$$

where ζ is the Riemann zeta function, or

$$\sigma_3(n) - \sigma_7(n) + 120\sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k) = 0.$$

In both of these examples, the input variable n ranges over many different values. However, interesting identities arise from even just two fixed input variables, which we denote n and r throughout this paper.

Theorem 2. *Let π be a prime, s be an integer relatively prime to π, α be a nonnegative integer such that $r = \pi^{\alpha}s$ and $n = \pi^{2\alpha+1}s$, and j be a fixed, nonnegative integer. Then the identity*

$$n^j\sigma_j(r) + r^j\sigma_j(r) = r^j\sigma_j(n), \tag{1}$$

is the unique algebraic identity in the variables n, r, $\sigma_j(r)$, and $\sigma_j(n)$, up to multiplication by a constant.

We then explore how (1) can be applied to perfect numbers, defined as integers n such that $\sigma(n) = 2n$. The standard forms for such numbers go back to Euler, who considered even and odd perfect numbers separately. An even number n is perfect if and only if

$$n = 2^a\left(2^{a+1} - 1\right), \tag{2}$$

where both a and $2^{a+1} - 1$ are prime, the latter being a Mersenne prime. Currently, 47 even perfect numbers are known [4], although it is not known whether the total count is finite or infinite. An odd perfect number would have to have the form

$$n = p^{\beta}t^2, \tag{3}$$

where p is prime, $(p, t) = 1$, and $p \equiv \beta \equiv 1 \pmod 4$. It is conjectured that no odd perfect numbers exist, and if one does exist it would have to be at least 10^{473} [5,2]. We combine these two forms into one, as follows.

Theorem 3. *If n is a perfect number, then*

$$n = \frac{r\sigma(r)}{2r - \sigma(r)}, \tag{4}$$

where r is a positive integer subject to one of the following three cases:

1. *If n is odd, then r is square.*
2. *If $n > 6$ is even, then $r = 2^a$ for some integer $a > 1$.*
3. *If $n = 6$, then either $r = 2$ or $r = 3$.*

Also, $\frac{n}{\sigma(r)}$ is integral for $r \neq 3$.

This reduces to either (2) or (3) if we choose n to be either even or odd, respectively.

2. Algebraic independence

We start with some preliminary lemmas. Let $S_k = \{x_0, \dots, x_{k+1}\}$ be a set of $k+2$ integer-valued functions for some $k \geqslant 0$. Define $g : \mathbb{Z}^+ \to (\mathbb{Z}^+)^{k+2}$ by

$$g(n) = \big(x_0(n), x_1(n), \dots, x_{k+1}(n)\big),$$

and $g_q : \mathbb{Z}^+ \to (\mathbb{Z}/q\mathbb{Z})^{k+2}$ for a prime q by letting

$$g_q(n) = \big(x_0(n), x_1(n), \dots, x_{k+1}(n)\big) \bmod q$$

be the reduction of $g(n)$ modulo q. The following two lemmas are clear.

Lemma 1. *Let P be a non-zero polynomial in $x_0, \dots, x_{k+1}$ with integer coefficients. If $P(x_0(n), \dots, x_{k+1}(n)) = 0$ for all $n \in \mathbb{Z}$ then $|g_q(\mathbb{Z}^+)| = O(q^{k+1})$.*

Lemma 2. *Suppose $\operatorname{ord}_q p$ divides z for a prime q, and suppose $j \geqslant 1$. Then*

$$\sigma_j\big(p^z\big) \equiv \begin{cases} z+1 \pmod q, & p^j \equiv 1 \pmod q, \\ 1 \pmod q, & \textit{otherwise}. \end{cases}$$

We now prove a third lemma, from which Theorem 1 follows.

Lemma 3. *Suppose we choose S_k to be the set of integer-valued functions*

$$\{I\} \cup \{\sigma_j\}_{j=0}^{k}.$$

Then there are infinitely many primes q such that $((\mathbb{Z}/q\mathbb{Z})^*)^{k+2} \subset g_q(\mathbb{Z}^+)$.

Proof. We will show how to choose $n = p_0^{e_0} p_1^{e_1} \cdots p_{k+1}^{e_{k+1}}$ such that $g_q(n)$ is any desired value of $((\mathbb{Z}/q\mathbb{Z})^*)^{k+2}$. Label the functions in S_k by setting $x_0 = I$, $x_i = \sigma_i$ for $0 < i \leqslant k$, and $x_{k+1} = \sigma_0$. Let $l = \operatorname{lcm}(\{1, \dots, k\})$, and let h be a prime which is relatively prime to l. Then choose q so $q \equiv 1 \pmod{hl}$. Note that this gives an infinite number of possibilities for q.

We proceed in $k+1$ steps. For the c-th step we choose the value of p_c and e_c, with p_c distinct from the primes chosen in all previous steps. This way, $g_q(n)$ is the componentwise product of $g_q(p_0^{e_0}), \dots, g_q(p_{k+1}^{e_{k+1}})$, since each $x_i \in S_k$ is multiplicative.

1. For $x_0 = I$, the first component of $g_q(p_0^{e_0})$ is congruent to $p_0^{e_0} \pmod q$. Then p_0 and e_0 can be chosen arbitrarily, with the restriction that $\sigma_i(p_0^{e_0}) \neq 0$ for all $i \geqslant 1$.
2. For each $x_i = \sigma_i$ with $1 \leqslant i \leqslant k$, choose p_i to have multiplicative order i in $(\mathbb{Z}/q\mathbb{Z})^*$, and choose e_i to be a multiple of i. Then by Lemma 2, $p_i^{e_i} \equiv 1$, $\sigma_j(p_i^{e_i}) \equiv 1$ for all $j < i$, and $\sigma_i(p_i^{e_i}) \equiv e_i + 1 \pmod q$. Since q is defined to be prime to i, the result $e_i + 1$ modulo q can be chosen arbitrarily, as long as $e_i \not\equiv -1 \pmod q$.
3. For $x_{k+1} = \sigma_0$, choose p_{k+1} to have multiplicative order h, where h is the same as in the choice of q, and choose e_{k+1} so $e_{k+1} \equiv h \pmod q$. Then $\sigma_0(p_{k+1}^{e_{k+1}}) = e_{k+1} + 1$, so we can choose $\sigma_0(n)$ arbitrarily. By Lemma 2, $p_{k+1}^{e_{k+1}} \equiv 1$ and $\sigma_i(p_{k+1}^{e_{k+1}}) \equiv 1$ for all $i \geqslant 1$.

This gives us a set of values such that the first c components of $g_q(p_c^{e_c})$ are 1. Therefore, by choosing the p_c's and e_c's for each value of c in order, we can construct $n = p_0^{e_0} p_1^{e_1} \dots p_k^{e_k}$ so that $g_q(n)$ is any arbitrary member of $((\mathbb{Z}/q\mathbb{Z})^*)^{k+2}$, and hence all of $((\mathbb{Z}/q\mathbb{Z})^*)^{k+2}$ is constructed. □

If we try to extend this to include $\varphi(n)$, however, we find that as a result of including primes p_c such that $p_c \equiv 1 \pmod{q}$ we get $\varphi(n) \equiv 0 \pmod{q}$. Including $\varphi(n)$ then would require a procedure more complicated than above.

3. Uniqueness of (1)

Let $\mathbb{Z}[F_j]$ be the ring of all polynomials with integer coefficients in the four variables $F_j = \{r, \sigma_j(r), n, \sigma_j(n)\}$. We want to show that the ideal of polynomials $f \in \mathbb{Z}[F_j]$ which vanish over U is principal and generated by (1).

For each prime q, define T_q to be the image of the map

$$(r, n) \mapsto \big(r, \sigma_j(r), n\big) \bmod q.$$

Lemma 4. *For infinitely many primes q, there are at least $q(q-1)^2$ distinct 3-tuples in T_q.*

Proof. Each element in T_q is the product of a 3-tuple of the form

$$\big(r, \sigma_j(r), r\big) \pmod{q}, \tag{5}$$

where $r \not\equiv 0 \pmod{q}$, and a 3-tuple of the form

$$\big(1, 1, \pi^{\alpha+1}\big) \pmod{q} \tag{6}$$

for a prime π and some $\alpha \geqslant 0$. Theorem 1 shows that there are infinitely many primes q so that there are at least $(q-1)^2$ elements of the form (5). Then, since we can multiply each such element by q elements of the form (6), we have a total of at least $q(q-1)^2$ distinct elements in T_q. □

Let $P(X_1, X_2, X_3, X_4) = X_1^j X_4 - (X_1^j + X_3^j)X_2$ as in (1). It is clear from direct calculation that $P(r, \sigma_j(r), n, \sigma_j(n)) = 0$ for all $(r, n) \in U$.

Lemma 5. *Let $R = \mathbb{Z}[X_1, X_2, X_3, X_4]$ be the ring of polynomials in X_1, X_2, X_3, and X_4 with integer coefficients. If there is a non-zero polynomial $Q(X_1, X_2, X_3, X_4) \in R$ so that $Q(r, \sigma_j(r), n, \sigma_j(n)) = 0$ for all $(r, n) \in U$, then Q is in the R-ideal generated by P.*

Proof. Suppose we consider P and Q in the larger ring $R[X_1^{-1}]$ which is the localization of R at $\{X_1^i\}_{i=0}^{\infty}$. We can write P as

$$P(X_1, X_2, X_3, X_4) = X_1^j\left(X_4 - \left(1 + \frac{X_3^j}{X_1^j}\right)X_2\right),$$

and we can rewrite the quotient ring $(R[X_1^{-1}])/(R[X_1^{-1}]P)$ as

$$\frac{\mathbb{Z}[X_1, X_1^{-1}][X_2, X_3, X_4]}{\mathbb{Z}[X_1, X_1^{-1}][X_2, X_3, X_4](X_4 - (1 + X_3^j X_1^{-j})X_2)} \cong \mathbb{Z}\big[X_1, X_1^{-1}\big][X_2, X_3].$$

This means we have $X_1^m Q = G + HP$ for some $G \in \mathbb{Z}[X_1, X_2, X_3]$, some $H \in R$, and some $m \geqslant 0$. Then for all $(r, n) \in U$,

$$\begin{aligned}0 &= r^m Q\big(r, \sigma_j(r), n, \sigma_j(n)\big)\\ &= G\big(r, \sigma_j(r), n\big) + H\big(r, \sigma_j(r), n, \sigma_j(n)\big) P\big(r, \sigma_j(r), n, \sigma_j(n)\big)\\ &= G\big(r, \sigma_j(r), n\big).\end{aligned}$$

For a prime q, $G \pmod q$ then vanishes at all 3-tuples in T_q. If G is not the zero polynomial, then for all sufficiently large q the number of zeros of $G \pmod q$ is bounded from above by a constant times q^2. But by Lemma 4, there are at least $q(q-1)^2$ elements of T_q for an infinite set of primes q. Therefore G must in fact be the zero polynomial, and so $X_1^m Q = HP$ for some $m \geqslant 0$. Because P is irreducible and $P \nmid X_1^m$, we get $P \mid Q$. □

4. Application to perfect numbers

We first note that our results on perfect numbers generalize the forms of Holdener [3], who shows that an odd number n is perfect if and only if

$$\frac{\sigma(n)}{n} = \frac{2\pi^\alpha(\pi-1)}{\pi^{\alpha+1}-1}.$$

Proof of Theorem 3. The sum of divisors function has the property that $\sigma(n)$ is odd if and only if n is square or twice a square. If n is perfect, then $\sigma(n) = 2n$ is even, and so n cannot be square. Therefore, we can suppose n is perfect in (1). By setting $j = 1$ and $\sigma(n) = 2n$ and then solving for n, we get (4).

First, suppose n is odd. Then π must be odd, and we can also write

$$\frac{\sigma(n)}{\sigma(r)} = \frac{2n}{\sigma(r)} = \frac{n+r}{r} = \pi^{\alpha+1} + 1,$$

which implies that $\frac{n}{\sigma(r)}$ is integral. Combining (3) and (1), we get $n = \pi^{2\alpha+1}s = p^\beta t^2$. We see that p is the only prime with an odd exponent in $p^\beta t^2$, so $p = \pi$, $\beta = 2\alpha + 1 \equiv 1 \pmod 4$, and $s = t^2$. It follows that α is even and so $r = \pi^\alpha s$ is square.

If n is even, we have two choices, since by (2) we can choose either $r = 2^a$ or $r = 2^{a+1} - 1$. In the first case, we can write

$$n = \frac{r\sigma(r)}{2r - \sigma(r)} = \frac{2^a(2^{a+1}-1)}{2^{a+1} - (2^{a+1}-1)} = 2^a\big(2^{a+1}-1\big)$$

which is just (2), and then $\frac{n}{\sigma(r)} = r$ is integral. In the second case,

$$\begin{aligned}\frac{\sigma(n)}{\sigma(r)} &= 2^{a+1} - 1 = r,\\ n &= \frac{r\sigma(r)}{2}.\end{aligned}$$

Therefore,

$$\begin{aligned}\frac{r\sigma(r)}{2} &= \frac{r\sigma(r)}{2r - \sigma(r)},\\ 2 &= 2r - \sigma(r),\\ 2 &= 2\big(2^{a+1}-1\big) - 2^{a+1},\end{aligned}$$

which we can solve to get $a = 1$, $r = 3$, and $n = 6$. We note, however, that in this case, $\frac{n}{\sigma(r)} = \frac{6}{4}$ is not integral. □

Acknowledgment

The author would like to thank Prof. Ted Chinburg of the University of Pennsylvania for his help and encouragement throughout the writing of this paper.

References

[1] R. Bellman, H. Shapiro, The algebraic independence of arithmetic functions (I) multiplicative functions, Duke Math. J. 15 (1948) 229–235.
[2] R.P. Brent, G.L. Cohen, H.J.J. te Riele, Improved techniques for lower bounds for odd perfect numbers, Math. Comp. 57 (1991) 857–868.
[3] J. Holdener, Conditions equivalent to the existence of odd perfect numbers, Math. Mag. 79 (2006) 389–391.
[4] Great internet mersenne prime search, http://www.mersenne.org, 2009a.
[5] Odd perfect number search, http://www.oddperfect.org, 2009b.